Department of Homeland Security Information Analysis and Infrastructure Protection Daily Open Source Infrastructure Report for 10 September 2003

Current Nationwide Threat Level is

ELEVATED
Significant Risk of Terrorist Attacks

For info click here
www.whitehouse.gov/homeland

Daily Overview

- The Associated Press reports federal agents are investigating how a man succeeded in stowing away in a cargo plane on a flight from New York to Dallas by shipping himself in a wooden crate. (See item 9)
- CBS reports Chicago's O'Hare airport has a security loophole: a back entrance where pilots, flight attendants, mechanics, vendors, luggage handlers and other airport personnel enter, without sufficient security screening. (See item 10)
- The Associated Press reports government investigators say fake IDs remain a huge security risk and the nation remains vulnerable to terrorists using false identification documents. (See item 21)

DHS/IAIP Update *Fast Jump*

Production Industries: Energy; Chemical; Defense Industrial Base
Service Industries: Banking and Finance; Transportation; Postal and Shipping
Sustenance and Health: Agriculture; Food; Water; Public Health
Federal and State: Government; Emergency Services
IT and Cyber: Information and Telecommunications; Internet Alert Dashboard
Other: General; DHS/IAIP Web Information

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *September 09, Capitol Media Services* — **Task force charged with reducing 'crisis mode'. Arizona Governor Janet Napolitano created a new task force on Monday, September 8, because "some of Arizona's infrastructure hangs by a critical thread," she told the committee.** The committee was appointed in the wake of last month's gasoline pipeline shutdown, which, coupled with consumer fears, resulted in long lines at Phoenix area gasoline

stations and sent prices skyrocketing not only in central Arizona but throughout the state and even the region. The governor acknowledged the panel may have only limited ability to force action that would prevent future problems could prove limited. That is because the two pipelines, both owned by Kinder Morgan Energy Partners, are federally regulated and do not answer to the state. She said, though, there may be things the committee can recommend on how to react when it reports in six months. That includes getting more and prompt information from the supplier −− in this case, the pipeline company −− and then keeping the public informed. **Technically, the governor charged the panel with looking at all potential shortages, including electricity, natural gas and water.** The governor said she sees the pipeline event as a chance to look at the larger question of how the state deals with such problems.
Source: http://www.azdailysun.com/non_sec/nav_includes/story.cfm?sto ryID=72752

2. *September 09, Associated Press* — **Regulators investigate possible design flaw at Oconee Nuclear Plant. The Nuclear Regulatory Commission said the backup cooling system at the Oconee Nuclear Plant near Seneca, SC, could get clogged with debris, choking the flow of water needed to cool the reactor.** Spokesperson Sandra Magee said Duke Energy, the operator of the plant, is making a dozen technical and procedural changes it will try to implement before the end of the year. She said that includes more inspections, "flushing" the system more often and additional training for operators.
Source: http://www.thecarolinachannel.com/andersonnewsroom/2466551/d etail.html

[Return to top]

Chemical Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

3. *September 08, American Forces Press Service* — **Army catamaran hauls equipment quickly.** The U.S. Army's newest experimental sea vessel is a heavy−lift catamaran called the Spearhead, hull number TSV−1X, which stands for "Theater Support Vessel − 1st Experimental." **Compared to the longtime Army workhorse vessel, the LSV, or Logistical Support Vessel, the TSV is four times faster at over 40 knots and can carry a more voluminous, though less heavy load,** said Anthony Dasig, a TSV engineer. The TSV moved the 101st Airborne Division military police from the Republic of Djibouti to Kuwait, making the 2,000−mile trip in two and a half days. The LSV would have needed 10 days to make the voyage and could only hold equipment, requiring the troops to fly separately, said Chief Warrant Officer Bill Slusher, the TSV navigation officer. **"The primary mission for the TSV is to lift soldiers with their equipment together, along with food, water and fuel,"** Slusher said. Another difference from the LSV is docking. With a shallow draft of 3.4 meters, the TSV can get into ports an LSV cannot. Since the vessel is experimental, the Army wants to know how it has performed in theater. Both enlisted and officer crew members meet regularly to conduct after−action reviews of the vessel's performance.

Source: http://www.defenselink.mil/news/Sep2003/n09082003_200309084. html

[Return to top]

Banking and Finance Sector

4. *September 09, Associated Press* — **U.S. readies colorful new $20 bills.** The first of America's green dollars to be colorized −− the $20 note sporting splashes of peach, blue and yellow −− will start appearing after October 9 in cash registers, ATM machines and wallets. **"This is the most secure note the United States has ever issued, and we want to get it out in circulation as quickly as we can," said Marsha Reidhill, assistant director for cash and fiscal agency for the Federal Reserve. The $20 bill is the most−counterfeited note in the United States.** The new $20 is the same size and still features the image of Andrew Jackson, the seventh president, on the front and the White House on the back. But along with the traditional green and black colors, the new notes also include faint touches of peach and blue in certain spots on the bills. Tiny number 20s are printed on the back of the notes in yellow. Besides color, the new notes include new features aimed making the bills harder to knock off. New, more colorful $50 and $100 bills −− the latter the most counterfeited note outside the country −− are expected in 2004 and 2005, respectively.
   Source: http://www.nytimes.com/aponline/business/AP−New−Money.html

5. *September 08, Associated Press* — **FBI suspects helpers in Pennsylvania bank robbery. Investigators said on Monday, September 8, they were confident a pizza deliveryman did not act alone when he robbed a bank with a bomb locked to his neck that went off moments later and killed him.** But whether Brian Douglas Wells was a willing participant or somehow "duped" into participating remained a mystery, FBI agent Bob Rudge said. **The idea that Wells acted alone is now the "least likely scenario and we are to the point where we have discounted that as a possibility,"** he said. Wells, 46, was stopped in his car, arrested and handcuffed on August 28 following a PNC Bank robbery near Erie, PA, but was killed when the bomb attached to a collar locked around his neck exploded while he and police waited for a bomb squad. Wells told police when he was arrested that someone had locked the bomb around his neck, started a timer on the bomb, forced him to rob the bank, and given a note with detailed instructions. **On Monday, investigators released a map of four locations listed in the note where Wells was allegedly supposed to receive further instructions. The two men seen darting through traffic were near locations mentioned in the note and are wanted for questioning,** authorities said.
   Source: http://abcnews.go.com/wire/US/ap20030908_2001.html

[Return to top]

Transportation Sector

6. *September 09, General Accounting Office* — **GAO−03−1155T – Maritime Security: Progress Made in Implementing Maritime Transportation Security Act, but Concerns Remain.** The General Accounting Office (GAO) today released this testimony by Margaret T. Wrightson, director, homeland security and justice, before the Senate Committee on

Commerce, Science, and Transportation. **The Senate Committee on Commerce, Science, and Transportation asked GAO to conduct a review of the status ofthe agencies' efforts to implement the security requirements of the act.** This testimony reflects GAO's preliminary findings; much of GAO's work in the area is still under way. **While much has been accomplished, GAO's review found five areas of concern.** Three relate primarily to security issues: • Only a limited number of ports covered by vessel identification system, • Questions about the scope and quality of port security assessments, and • Concerns related to approving security plans for foreign vessels. Two relate primarily to organizational and operational matters: • Potential duplication of maritime intelligence efforts, and • Inconsistency with Port Security Grant Program requirements. Highlights:
http://www.gao.gov/highlights/d031155thigh.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−03−1155T

7. *September 09, General Accounting Office* — **GAO−03−1154T – Transportation Security: Federal Action Needed to Enhance Security Efforts.** The General Accounting Office (GAO) today released this testimony by Peter Guerrero, director, physical infrastructure, before the Senate Committee on Commerce, Science, and Transportation. **GAO was asked to examine the challenges in securing the transportation system and the federal role and actions in transportation security.** In a June 2003 report, GAO recommended that TSA and DOT use a mechanism, such as a memorandum of agreement, to define and clarify each entity's role and responsibilities in transportation security matters. **Based on the uncertainty in the entities' roles and responsibilities, GAO continues to believe its recommendation is valid and would help address transportation security challenges.** Highlights:
http://www.gao.gov/highlights/d031154thigh.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−03−1154T

8. *September 09, Washington Post* — **Fliers may be rated for risk level.** In another move to protect air travelers, the federal government and the airlines will phase in a computer system next year to measure the risk posed by every passenger on every flight in the United States. **The Transportation Security Administration (TSA) will seek to compare personal information against criminal records and intelligence information. Passengers will be assigned a color code −− green, yellow or red −− based in part on their city of departure, destination, traveling companions and date of ticket purchase.** Most people will be coded green and sail through. But up to 8 percent of passengers who board the nation's 26,000 daily flights will be coded "yellow" and will undergo additional screening at the checkpoint, according to people familiar with the program. An estimated one to two percent will be labeled "red" and will be prohibited from boarding. These passengers also will face police questioning and may be arrested. **The system "will provide protections for the flying public," said TSA spokesman Brian Turmail. "Not only should we keep passengers from sitting next to a terrorist, we should keep them from sitting next to wanted ax murderers."** If all goes as planned, the TSA will begin the new computer screening of some passengers as early as next summer and eventually it will be used for all domestic travelers.
Source: http://www.washingtonpost.com/wp−dyn/articles/A45434−2003Sep 8.html

9. *September 09, Associated Press* — **FBI probes man who shipped himself to Dallas. Federal agents say they are investigating how a man succeeded in stowing away in a cargo plane on a flight from New York to Dallas by shipping himself in a wooden crate.** After hours of

traveling, Charles McKinley, 25, of New York City, pried open the crate with a crowbar Saturday morning, authorities said. He popped up outside his parents' doorstep in suburban DeSoto, shook the hand of a shocked deliveryman and walked away, The Dallas Morning News reported Tuesday. The deliveryman called DeSoto police, who arrested him on outstanding Texas warrants. McKinley has not been charged with a crime, officials said. **The FBI and the Transportation Security Administration are investigating. "It's amazing that the gentleman survived. It's absolutely a bizarre case," said FBI Special Agent Lori Bailey, a spokeswoman for the Dallas field office. "Our concern at this point is to determine how this was done."** Officials said McKinley's crate was put aboard a pressurized Boeing 727 operated by Indiana−based Kitty Hawk Cargo from Kennedy International to Fort Wayne, Ind. The crate was transferred to a second plane bound for Dallas−Fort Worth International. A ground shipping company picked up the crate and delivered it to the residence of McKinley's parents.
Source: http://www.fredericksburg.com/News/apmethods/apstory?urlfeed =D7TF0AI80.xml

10. *September 09, CBS 2 Chicago* — **Threat at airport's back door. Aviation expert and former American Airlines pilot Jim Tilmon has uncovered some unsettling security concerns about security at Chicago's O'Hare airport.** Although passengers are thoroughly screened, a little known security loophole exists through the back door of the airport, a weak link that could potentially be used by a terrorist to create an aviation disaster. There is a back entrance, known as the employee parking lot at O'Hare Airport used by pilots, flight attendants, mechanics, vendors, luggage handlers and other airport personnel. **As observed by CBS cameras, employees hand over their airport ID's and are waved on by the guards. No trunks are opened, nor are bottoms of cars checked. At this same employee entrance, CBS cameras caught vendor and construction trucks being waved through without being searched. This, according to Commissioner Walker, is a clear security violation. All trucks are supposed to be screened at the gate.**
Source: http://cbs2chicago.com/special/local_story_252112858.html

[Return to top]

Postal and Shipping Sector

11. *September 09, Associated Press* — **Postal Service finances. The U.S. Postal Service expects to end this fiscal year $4.2 billion in the black, allowing it to pay down a substantial amount of debt, the agency said Tuesday.** Chief Financial Officer Richard Strasser said the financial plan is to reduce debt by $3.8 billion this year to $7.3 billion. **In addition, the agency expects a $2.1 billion net income for the 2004 fiscal year, which begins in October, allowing further reduction in debt, Strasser told the agency's Board of Governors.** Strasser said the post office expects to finish this fiscal year with revenue of $68.9 billion, $1.5 billion less than planned, and spending of $64.7 billion, $1.8 billion less than expected. Overall mail volume decreased to 202 billion pieces and the mix has changed with a drop in first−class mail, Strasser said. He forecast a continued increase in advertising mail. At the same time the post office is delivering to an added 1.8 million homes, businesses and postal boxes annually, rising to total 143 million in 2004. **In addition to last year's rate increase, Strasser noted that the agency has increased automation and cut staff to save money. From 1999 through 2004, he noted, the agency will have cut 74,000 full−time and about 10,000 part−time workers.**

Source: http://wcco.com/finance/finance_story_252153337.html

[Return to top]

Agriculture Sector

12. *September 09, USAgNet* — **GM plot vandalized. A biotech filed of corn in France, owned by Monsanto, has been attacked and destroyed. Police would not speculate who was behind the attack, but added that it had occurred a few hours after an anti−biotech demonstration on Friday. Another of Monsanto's genetically modified (GM) fields, also in the southwest of France near Toulouse, was destroyed in July.** France and other European countries have resisted using the new genetic technology in agriculture. France grows experimental GM crops on around 100 sites, all approved by the farm ministry.
Source: http://www.usagnet.com/news−search.cfm?Id=964

13. *September 09, Illinois Ag Connection* — **Researchers locate sources of resistance to soybean aphids. In recent weeks, soybean aphids have suddenly emerged as a major concern for growers throughout the Midwest.** Densities of several thousand aphids per plant have been reported in many fields across the area. The aphids were first discovered in large numbers in soybean fields near the end of the 2000 growing season. After careful scientific investigation, they were identified as Aphis glycines, which had previously been reported only in Asia, Australia, and some Pacific islands. **Researchers from the National Soybean Research Laboratory at the University of Illinois, however, have recently discovered three soybean lines with strong resistance to the aphids which could eventually be incorporated into new commercial varieties. "Once the aphids infest a field, the most common means of control is to spray the field with an insecticide that can cost 20 to 25 dollars per acre or more," said Glen Hartman U.S. Department of Agriculture plant pathologist.** "If resistant commercial varieties were available, the savings to growers could be substantial."
Source: http://www.illinoisagconnection.com/story−state.cfm?Id=690&y r=2003

[Return to top]

Food Sector

14. *September 08, AScribe Newswire* — **Food security.** Responding to the events of September 11, 2001, Congress passed the Public Health Security and Bioterrorism Preparedness and Response Act of 2002. The Bioterrorism Act takes effect on December 12, 2003, providing new and refurbished legislation to protect the nation's food supply. **While most food firms recognize the need for guidelines that protect the U.S. food system against a possible bioterrorist attack, a Food Policy Institute (FPI) study at Rutgers University suggests that many food firms are not prepared for the new Food and Drug Administration (FDA) rules.** The study also indicates that food firms believe that complying with the Bioterrorism Act may be challenging. A small and diverse group of food industry executives convened at the FDA telecasts last spring to learn about proposed regulations for the Bioterrorism Act. Their post−telecast responses on the four sections reveal that 60 percent of stakeholders generally do not know what to expect from the Bioterrorism Act and the remaining expect that compliance

will pose a "moderate to significant burden" on their businesses. Seventy−seven percent feel the act has or will lead to increased food security, and are confident that food system security will increase with the act in place than without.
Source: http://www.ascribe.org/cgi−bin/spew4th.pl?ascribeid=20030908.112751&time=13%2000%20PDT&year=2003&public=1

[Return to top]

Water Sector

15. *September 09, WaterTech Online* — **Bioremediation an effective alternative for cleanups.** Bioremediation is a relatively new process that uses bacteria to neutralize pollutants in wastewater treatment or transform them to harmless chemical products. **Bioremediation has proven to be an important remediation technology for three main reasons. First, the procedure uses naturally occurring biogeochemical processes to power the cleanup.** This process typically involves stimulating native bacteria in the contaminated area, with the bacteria actually destroying the contaminants. **Secondly, bioremediation destroys or immobilizes contaminants rather than transferring them from one place to another.** For example, some treatments liberate contaminants from the soil, only to release them into the air where the chemicals pollute the atmosphere. **Finally, bioremediation conserves limited financial resources due to shortened cleanup times and/or lower capital expenditures relative to many other remediation technologies.** The biostimulant is often easily available at a low cost making the process speedy and cheap.
Source: http://www.watertechonline.com/news.asp?mode=4&N_ID=42805

[Return to top]

Public Health Sector

16. *September 09, University of Chicago Medical Center* — **Physician bioterror survey. A survey of 1,000 physicians found that four out of five were willing to care for victims of a bioterrorist attack, but only one out of five felt well prepared for such a role.** The researchers were just as troubled by the 20 percent who were unwilling as by the 80 percent who were unprepared. Fewer physicians reported a willingness to treat as the authors described scenarios of increased personal risk. **Although 80 percent were willing to treat patients with an "unknown but potentially deadly illness," that fell to 40 percent when the question involved a risk of "contracting a deadly illness." It dropped to 33 percent when the virus was specified as smallpox and it was stipulated that the physicians had not first been vaccinated.** "Given the complexities of learning about bioterrorism, the perceived low likelihood of a local attack, and the many competing priorities facing doctors, it might be unrealistic to expect most physicians to learn how to detect and treat even the most likely bioterror agents," noted the authors. "Efforts to strengthen the public health infrastructure and ensure that all physicians understand their role in the emergency response system may be equally important ways of fostering preparedness."
Source: http://www.eurekalert.org/pub_releases/2003−09/uocm−mpw09050 3.php

17. *September 09, CNN* — **Health care costs increasing. Premiums for employer−sponsored health insurance increased almost 14 percent between spring 2002 and spring 2003, the highest increase since 1990, according to a survey released Tuesday by the Kaiser Family Foundation and Heath Research Educational Trust.** Although employers continue to foot most of the insurance bill, they are steadily passing on higher costs to their employees. **Since 2000, that annual premium paid by employees to insure themselves and their families has increased nearly 49 percent.** Nearly four in five workers must pay a deductible before their health plans will pick up any expenses. Under a conventional health plan, workers paid an average deductible of $384 (up 30 percent since last year) for single coverage and $785 (up 12 percent) for family coverage. A saving grace for employees with large medical bills is an annual cap on the total out−of−pocket expenses they are expected to pay. Yet, 15 percent of all plans report that they are reducing the services or items included under that limit.
Source: http://money.cnn.com/2003/09/09/pf/insurance/employerhealthp lans/

18. *September 09, Reuters* — **New step urged to curb biological weapons threat.** At a British Association science conference on Tuesday, September 9, an expert from the University of California, Davis, Mark Wheelis, said that existing intelligence was inadequate and an international inspection system might be needed to lessen the threat and prevent a new biological arms race. **Malcolm Dando, a professor at Britain's Bradford University, said the simplification of technologies which could be misused meant small groups and deranged individuals could also pose a threat and cause mayhem. The experts agreed that it was unclear what would happen in the event of a biological attack and whether any warning would be given before or after an attack.** They suspected the first sign was likely to be people becoming ill, but scientists would only be able to spot an attack by mapping the spread of the disease. "There are a range of different scenarios that are possible and it isn't clear how these things will pan out," said Alastair Hay, a professor at Britain's Leeds University, adding that a chemical incident would be easier to map than a biological one.
Source: http://www.reuters.com/newsArticle.jhtml?type=topNews&storyI D=3415222

19. *September 08, Reuters* — **Canada hosts test on possible smallpox outbreak. Some of the world's leading nations opened a three−day exercise on Monday that will assess how the international community would deal with an outbreak of smallpox, officials said.** The exercise, dubbed Operation Global Mercury, aims to help improve emergency preparedness. Canada is running the exercise, which involves a total of around 250 officials in France, Germany, Italy, Japan, Mexico, Britain, the United States, and at the European Commission. **"(It)...will take place in a compressed time frame of 56 hours representing a series of fictitious events experienced over a period of 12 days as a result of an outbreak of smallpox," said a Canadian health ministry statement. "The aim of the exercise is to evaluate international communications exchanges and record the responses between participating countries and organizations during a public health emergency such as an outbreak of smallpox."**
Source: http://www.alertnet.org/thenews/newsdesk/N08331860.htm

[Return to top]

Government Sector

20. *September 09, Reuters* — **U.S. offers extension on new passport rules.** The United States has offered to extend by one year the target date for tightening the rules for letting people enter the country without visas, a State Department official said on Tuesday. **Taking effect October 1, those whose passports are not readable by machine would not be able to enter the United States without visas, even if they come from one of the 27 countries that are part of a visa waiver program. But the State Department, recognizing that many passports are still not machine−readable, has told 26 of the governments that they can apply for an extension of about one year.** The countries in the visa waiver program are mostly affluent democracies whose citizens are thought unlikely to seek work in the United States illegally. They include most of Western Europe, Japan, Australia, New Zealand and Singapore. Belgium, which is under special rules, cannot apply for the extension. The requirement of machine−readability has applied to Belgium since May because of U.S. concerns about the security of Belgian passports, the official said. **Foreign governments in the visa waiver program face another deadline on October 26, 2004, by which date the United States wants them to introduce "biometric identifiers" in passports they issue.** The identifiers, which could be in the form of computer microchips, would include digitally coded information about the person's facial features or fingerprints.
Source: http://www.cnn.com/2003/TRAVEL/09/09/passport.rules.reut/ind ex.html

21. *September 09, Associated Press* — **Fake IDs remain huge U.S. security risk. The nation remains vulnerable to terrorists using false identification documents, say government investigators who say they were permitted to drive a truck into a Justice Department courtyard using false identification cards.** "Unless action is taken, individuals who want to cause harm can easily exploit these vulnerabilities," Robert Cramer, who directs special investigations for the General Accounting Office, told the Senate Finance Committee Tuesday. GAO investigators visited driver's license agencies in several states and were able to obtain driver's licenses using forged documents, including counterfeit out−of−state licenses. **Asa Hutchinson, the undersecretary for border security at the Department of Homeland Security, noted that 60,000 fraudulent documents have been confiscated at borders this year, and said training is being enhanced so agents will spot false documents. But he said the country has more than 240 different types of license** Youssef Hmimssa, who lived with members of a terrorist cell in Detroit and later helped the government convict several of them on terrorism charges, told the committee he easily obtained Social Security numbers, driver's licenses and even a U.S. passport after moving to Chicago in 1994 on a false French passport. **James Lockhart, deputy commissioner of Social Security, responded that his agency is now verifying any documents filed by immigrants with the Department of Homeland Security before providing a Social Security number.**
Source: http://www.newsday.com/news/politics/wire/sns−ap−terrorism−f ake−ids,0,6074562.story?coll=sns−ap−politics−headlines

[Return to top]

Emergency Services Sector

22. *September 09, National Journal's Technology Daily* — **First responders need national standards, says former lawmaker.** Local "first responders" to emergencies will not be able to effectively react to a terrorist attack until they have a standard for response, a former senator

said on Tuesday. **"What we need is a mandate for national minimum standards for homeland security for first responders," former Republican Sen. Warren Rudman, NH, told members of the House Government Reform Subcommittee on National Security, Emerging Threats and International Relations. "You cannot establish priorities until you know what the standards are."** More specifically, Rudman suggested that the Homeland Security and Health and Human Services departments work to set the standards, and that Homeland Security institute a "best practices" guide on how to work with state and local governments. John Tierney, D−MA, said first responders in his district could use national standards. Subcommittee Chairman Christopher Shays, R−CN, agreed that the nation needs standards but stressed that we cannot "afford to wait for a national consensus on standards to emerge before funding critical first−responder initiatives."
Source: http://www.govexec.com/dailyfed/0903/090903td2.htm

[Return to top]

Information and Telecommunications Sector

23. *September 09, New York Times* — **Cellphone companies agree to set of consumer guidelines. The nation's largest cellular phone companies announced a voluntary seal−of−approval program Tuesday, September 9, in hopes of staving off more restrictive consumer legislation**. The national wireless carriers−−Verizon Wireless, Cingular, Sprint PCS, Nextel and AT&T, along with numerous regional companies−−have agreed to adhere to a 10−part code of behavior that is intended to make it easier for consumers to compare prices and plans. **All companies that display the seal must provide a minimum 14−day trial period for new customers, coverage maps describing where service is available, and specific disclosure of rates and plans, among other things**. Packaging and documents from the companies will be displaying the Seal of Wireless Quality/Consumer Information within a few weeks, and several companies are already adhering to the guidelines. The Cellular Telecommunications and Internet Association in Washington, the trade group for the wireless industry, said it would conduct annual audits to assure that companies displaying the seal are in compliance.
Source: http://www.nytimes.com/2003/09/09/technology/09CELL.html

24. *September 09, Reuters* — **New York Times hacker surrendered, booked.** Hacker Adrian Lamo, 22, turned himself in to federal authorities in Sacramento, CA, on Tuesday, September 9, to face charges related to breaking into the internal network of The New York Times newspaper. Lamo could face fines and prison time under the Computer Fraud and Abuse Act of 1986, which outlaws unauthorized access to computer networks. **Lamo hacked into the New York Times network in February 2002 and accessed employee records, phone numbers, and Social Security numbers of editorial page contributors**. In the past Lamo has also discovered holes in corporate networks of Excite@Home Corp., Yahoo Inc., and WorldCom, among others, often through laser printers and other unlikely entry points. Lamo's defense is likely to be the "white−hat hacker" defense, said Mark Rasch, former head of the computer crime unit at the U.S. Department of Justice. White−hat hacker is a term used for people who work to protect computers from attack while "black−hat hackers" are those who attempt to break into them. However, **the law focuses on the intent to break into the computer, not the motive**, said Rasch.
Source: http://asia.reuters.com/newsArticle.jhtml?type=internetNews& storyID=3414987

Internet Alert Dashboard

Current Alert Levels

AlertCon: 1 out of 4 https://gtoc.iss.net	Security Focus ThreatCon: 1 out of 4 http://analyzer.securityfocus.com/

Current Virus and Port Attacks

Virus:	#1 Virus in the United States: **WORM_SOBIG.F** Source: http://wtc.trendmicro.com/wtc/wmap.html, Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States]
Top 10 Target Ports	135 (epmap), 137 (netbios−ns), 1434 (ms−sql−m), 111 (sunrpc), 443 (https), 445 (microsoft−ds), 80 (www), 554 (rtsp), 139 (netbios−ssn), 1433 (ms−sql−s) Source: http://isc.incidents.org/top10.html; Internet Storm Center

[Return to top]

General Sector

25. *September 10, Herald Sun (Australia)* — **Security fears as laptop stolen.** Highly sensitive government security information has been stolen in a second major intelligence breach. **Australian Federal Police are investigating the theft of a laptop computer containing details of national maritime security. The Canberra break−in – five days before Customs computers were stolen from Sydney airport last month – comes amid concerns terrorists are hunting top−secret information.** The Herald Sun can reveal thieves used an electronic swipe card to break into the Department of Transport's Canberra headquarters before forcing their way into the security section. **The main prize was the laptop computer, which contained a Powerpoint presentation on national maritime security. Port security has emerged as a major priority amid fears containers could be used to smuggle deadly biological or radiological weapons across Australia's borders.** The Government is preparing to spend $100 million terror−proofing hundreds of container terminals and bulk−handling terminals nationwide. The early−morning break−in on August 22 was described by a source as a well planned operation by people who knew the department office layout intimately. Source: http://www.theadvertiser.news.com.au/common/story_page/0,5936,7222941%5E421,00.html

26. *September 09, Associated Press* — **Several Israelis die in two bombings hours apart. Twin Palestinian suicide bombings −− one at a bus stop crowded with soldiers near Tel Aviv, the second five hours later at a popular Jerusalem nightspot −− killed at least 14 Israelis and wounded and maimed dozens as the region grappled with a new wave of savage bloodletting.** There were no claims of responsibility, but the Islamic militant group Hamas,

which has carried out most of the roughly 100 suicide bombings against Israelis over the last three years, had been expected to avenge Israel's attempt on the life of its spiritual leader on Saturday. **The first bombing came about 6 p.m., as soldiers were waiting for rides home outside the Tsrifin army base near the Tel Aviv suburb of Rishon Letzion. More than five hours later, about 11:20 p.m., another suicide bomber entered the Hillel Cafe, a popular bistro in the posh German colony neighborhood of Jerusalem.** At least six other people were killed and more than 30 were wounded, rescue workers said.
Source: http://www.nytimes.com/aponline/international/AP−Israel−Pale stinians.html?hp

[Return to top]

DHS/IAIP Products &Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP web−site (http://www.nipc.gov), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Warnings − DHS/IAIP Assessements, Advisories, and Alerts: DHS/IAIP produces three levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact.

DHS/IAIP Publications − DHS/IAIP Daily Reports, CyberNotes, Information Bulletins, and other publications

DHS/IAIP Daily Reports Archive − Access past DHS/IAIP Daily Open Source Infrastructure Reports

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 703−883−6631
Subscription and Distribution Information	Send mail to nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 703−883−6631 for more information.

Contact DHS/IAIP

To report any incidents or to request information from DHS/IAIP, contact the DHS/IAIP Watch at nipc.watch@fbi.gov or call 202−323−3204.

DHS/IAIP Disclaimer